

Sécurité des Systèmes Industriels Interconnectés

Approche ferroviaire :

Cas d'une coupure entre un courant Managérial et le Terrain en France depuis les années 50

1. Introduction

Notons avec Caire (2014, résumé p. 1/13) que « *la cybersécurité des systèmes industriels est devenue un enjeu majeur qui conduit les États à établir de nouvelles réglementations, applicables en premier lieu aux systèmes critiques. Or ceux-ci répondent déjà à des exigences élevées de sûreté de fonctionnement, qui sont satisfaites par la mise en œuvre de processus de développement et d'assurance particuliers, permettant leur homologation. Ces processus s'appuient sur un ensemble de méthodes et techniques rigoureuses et formalisées. La question est alors d'intégrer la cybersécurité dans les démarches de sûreté.* »

Et avec Dechy et al. (2010) « *pour une culture des accidents au service de la sécurité industrielle* », on rappelle certaines des raisons qui ont amenés à la culture de sûreté. La première, « *la nouvelle accidentologie et la culture des accidents, par la nature des enseignements qu'elles proposent, doivent contribuer au nécessaire changement de paradigme. La seconde est de répondre opérationnellement à la problématique du transfert de connaissance des accidents.* » Selon Dechy et al. il semble « *nécessaire de doter les acteurs des organisations à hauts-risques des moyens de développer une mémoire collective et vivante à partir des connaissances des accidents.* »

En effet pour le cas de la cybersécurité, « *le déploiement du malware Stuxnet, puis les révélations sur certaines réflexions stratégiques sur le cyberspace..., ont montré que des cyberattaques capables d'infliger des destructions matérielles sur des systèmes industriels sont une menace avérée, constituant de fait un nouvel enjeu de sécurité,* » Caire (2014, p.2/13),

C'est ainsi que la conséquence d'une attaque de la Sécurité de Système Informatique peut être fatale pour la Sécurité des Systèmes Industriels

Interconnectés, SSII. Et avec Garandel et Périnet (2014, p. 1/6) on note que « *les accidents mettent à l'épreuve nos présupposés sur la sécurité, bousculant potentiellement nos grilles de lecture et nos registres d'actions habituels. Ces accidents imposent aux organisations un exercice de réflexivité, comprenant à la fois une part d'appropriation de l'accident survenu et une part essentielle d'introspection et d'évaluation de nos « défenses »* ».

Ainsi pour les SSI avec la Sécurité des Systèmes Industriels Interconnectés, « *quels que soient les types de changements ou de transformations, comment appréhender les risques, comment les prévenir, comment les traiter* » ? « *Comment s'assurer de la pertinence du processus de maîtrise des risques tout au long du cycle de vie dans un contexte où tous les paradigmes peuvent être peu ou prou remis en cause ? Quand et comment parler de « résilience aux changements » ?...* (Lardeux, 2015, p. 2/6) »

Dans l'industrie de production de projets informatiques, initialement la théorie des organisations semblerait avoir été commune (Caire, 2014, résumé p. 1/13). Pour la SSI, avec les SSII, les concepts évoluent et les acteurs changent depuis l'origine, encore plus depuis les années 2000. Ce qui pose un problème d'évolution :

- de ces systèmes au regard d'objectifs de coordination de projet ;
- des fondamentaux de la pensée organisationnelle avec (une épistémologie débouchant sur une ontologie de) ces systèmes ;
- épistémologique de la théorie des organisations.

2. Quelques aspects de revue de littérature

L'inattendu est l'affaire de la sécurité informatique et est ici induite par une réflexion, comme culture de sécurité – sûreté (Lardeux, 2015, p. 2/6) vs HFO, Haute Fiabilité Organisationnelle (ou HRO, High Reliability Organizational).

La fiabilité comme la sécurité sont des concepts de, et avec la sûreté de fonctionnement (Arlat et al., 2006). Avec Caire (2014, p.2/13) notons que « *sur le plan méthodologique, les questions de sûreté et de cybersécurité ne sont pas séparables en raison de la complexité intrinsèque des systèmes informatiques industriels, si bien qu'elles ne peuvent faire l'objet de traitements conçus et mis*

en œuvre indépendamment l'une de l'autre. » ... Et, « avant de déterminer précisément les exigences que devra satisfaire le cycle de vie de Sécurité globale, il est important d'établir une comparaison entre la sûreté de fonctionnement et la cybersécurité. » ... De plus « pour répondre à l'exigence de cohérence du cycle de vie de Sécurité globale, il faut disposer d'une méthode d'analyse des risques induits par la malveillance aussi rigoureuse et structurée que les méthodes de la sûreté, » (Dechy, 2010).

En fait, ce procédé relève du déterminisme, et les chercheurs de la HRO soulèvent un paradoxe selon lequel ils *« défendent l'idée que les organisations qui soutiennent une fiabilité élevée de leurs opérations, sont simultanément capables de maintenir des routines invariantes et de faire face à des fluctuations inattendues, afin d'éviter tout résultat indésirable et potentiellement catastrophique, »* Roux-Dufort (Vidaillet, 2003, 2013, p. 139/185).

De plus Weick, Sutcliffe et Obstfeld (1999) introduisent de nouvelles réflexions sur ce paradoxe ; ainsi *« pour qu'un système reste fiable, il doit d'une façon ou d'une autre gérer des situations imprévues d'une manière qui anticipe des conséquences inattendues. C'est ici que les définitions existantes de la fiabilité sont trompeuses. »*

Pour Bierly et Spencer (1995) et Schulman (1993) *« ce paradoxe reste au cœur des discussions sur la fiabilité. »* Pour Roux-Dufort ces recherches *« assimilent la fiabilité à une absence de variation dans la performance. »* .. ainsi *« des processus constants, »* compris ici comme suites d'actions sans variation possible, *« ne peuvent traiter ce qu'ils n'anticipent pas. L'idée que les routines invariantes seraient une source de fiabilité réunit les variations et la stabilité et rend les mécanismes de performance fiables en situation dégradée, »* avec la SSII encore *« plus difficiles à comprendre, (Vidaillet, 2003, 2013, p. 139/185) ».*

Ainsi dans la production de projets informatiques en France, dans le fil de Roux-Dufort, on note que *« construire une théorie sur la fiabilité organisationnelle exige de résoudre ce paradoxe, à un moment où des recherches tendent à montrer empiriquement que la fiabilité est plus une affaire de traitement de l'inattendu que de préserver des processus routiniers des organisations. »*

Pour un cheminement au regard de la Sécurité des Systèmes Industriels

Interconnectés vs fiabilité et fiabilité organisationnelle, avec Roux-Dufort l'on comprend que « *trois courants de recherche ont contribué à éclairer le paradoxe de la fiabilité : l'école des HRO, la théorie des accidents normaux, le courant de gestion des crises.* »

De plus « *ces courants ont contribué à identifier les facteurs de fiabilité, soit en détectant les conditions organisationnelles qui assurent que les organisations à hauts risques en situation normale ne produisent que très peu d'erreurs catastrophiques (Roberts, 1990, 1993), soit en mettant en évidence les processus qui génèrent des accidents et des catastrophes dans ces organisations (Perrow, 1994, Pauchant et Mitroff, 1992, Shrivastava, 1992, Pearson et Clair, 1998)....* » ce qui va nous aider pour la Sécurité des Systèmes Industriels Interconnectés.

Mais selon Roux-Dufort en « *se focalisant sur les structures et l'organisation, ces trois courants sous-estiment le rôle critique que les groupes et les individus pourraient jouer dans les réajustements et gestion des échecs.* »

De plus, avec Caire (2014, p.2/13) en insistant « *sur le plan méthodologique, les questions de sûreté et de cybersécurité* » on sous-estime la question de la culture d'organisation (Pesqueux, 2002, p. 313/396 ; Le modèle culturel de l'organisation).

De fait avec Dechy et al. il « *est intéressant de noter que la notion de culture s'intéresse à des groupes et non à des individus.* » Et il mentionne un glissement « *lorsque l'on se réfère à la culture de sécurité, ou à son usage par une partie du management, il est rapidement fait référence à un « état d'esprit » qui s'adresse plus particulièrement à des individus. (Hopkins, 2002). Les événements dus à des manques ou des faiblesses dans la culture de sécurité pourraient trouver leurs racines dans des défauts « d'état d'esprit ».* Hopkins souligne que « *la culture en tant qu'état d'esprit tend à ignorer les conditions latentes qui sous tendent tous les accidents du travail, en mettant en cause, à la place, les attitudes des opérateurs comme cause des accidents* » (Hopkins, 2002). »

Et bien sûr avec la question de la Sécurité des Systèmes Industriels Interconnectés « *les relations de travail modifient les comportements des acteurs individuels et à leur tour sont modifiées par eux. Si des changements significatifs interviennent dans l'environnement dans lequel acteurs individuels et organisations se trouvent, ils peuvent déstabiliser l'équilibre des acteurs et provoquer chez eux des pertes de*

sens fondamentales (Weick, 1995) ; l'effondrement des rôles acquis peut empêcher, à la limite, toute tentative d'adaptation et d'élaboration de nouvelles capacités d'organisation de leur part (Koënik, 1996), » (Artaza Abaroa, 2006, p. 2/31).

Si l'exercice paraît plus clairement énoncé, il n'en demeure pas moins complexe. En effet, les rapports d'enquête réalisés suite aux accidents technologiques majeurs montrent que « *les accidents ne se produisent pas en conséquence d'une seule erreur ou d'une simple défaillance technique, mais en conséquence d'une série d'événements, de décisions, d'erreurs d'appréciations et d'omissions se traduisant par un échec systémique. Cette réalité doit conduire les analystes à convoquer une variété la plus importante possibles de thèmes, afin d'offrir plus d'opportunités pour progresser* » » (Garandel, Périnet, 2014, p. 6/7 (Deepwater Horizon, 2010 ; Columbia, 2003).

Avec Weick, « *d'autres facteurs concourant au maintien de la fiabilité, tels que l'existence d'une culture de vigilance généralisée ou le « story-telling effect ». Cadre où Weick contribue à identifier de nouvelles caractéristiques des HROs, plus centrées sur la qualité des interactions et les processus mentaux collectifs, tels qu'une (1) attention aux dysfonctionnements, une (2) réticence à simplifier les interprétations, une (3) sensibilité à l'égard des opérations, un (4) engagement dans la résilience, un (5) respect de l'expérience (Weick et Sutcliffe, 2007), » (Tillement, 2011, p. 67/551).*

Deux concepts de construction de la fiabilité organisationnelle, qui ont des conséquences sur la sécurité informatique, et sont « *particulièrement centraux : celui de (I) vigilance collective et celui de (II) résilience organisationnelle. »*

Avec la vigilance collective, les actions, la dynamique, les réactions et interactions font émerger du sens, des pistes à la fois testées, conservées et/ou éliminées pour d'autres plus sûres à leur tour en faisant tout en étant tous collectivement vigilants sur la question de la sécurité informatique (Tillement, 2011, p. 68/551).

Avec Hollnagel et Woods (2006) » qui « *partagent la vision dynamique de la sécurité, et considèrent comme normales et nécessaires la variabilité, ils ont largement contribué à étayer le concept de résilience. C'est le cas des fondateurs de l'ingénierie de la résilience, mais aussi de ceux qui se sont intéressés aux fondements de la robustesse organisationnelle (Boissières, 2005 ; Terssac et al.,*

2009), » (Tillement, 2011).

Mais on mesurerait la production de projets, informatiques, par des représentations sous la forme de modèles mathématiques et de modèles d'organisations (Pesqueux, 2002, p. 11/396). Cependant qu'à "*l'atelier*" aucun calibre, ni méthode ne conviennent totalement. Alors, résilience oblige (!!), on y opère par glissements de modèles vers d'autres, émergents alors ; bricolage, mieux encore, ajustement par ajustages de mises en pratiques de concepts par liens-disjonctions-continuum.

En d'autres termes, pour ce qui est de la SSI, pour éviter la crise dans la production de projets informatiques en France, l'organisation est dans une logique de système sociaux-technique structurante. Mais du fait d'une indépendance entre la conceptualisation de la performance organisationnelle et celle de la performance technique, il émerge un problème de conceptualisation sur la notion de performance organisationnelle. L'évaluation de nouvelles approches au détriment d'anciennes aboutit à une sédimentation par rapport à une institutionnalisation avec la question de la Sécurité des Systèmes Industriels Interconnectés.

Tout a un rendement très élevé ou exceptionnel recherché ici pour la Sécurité des Systèmes Industriels Interconnectés. Plus encore, on recherche toujours une amélioration, un perfectionnement possible du point de vue de la performance avec ces systèmes industriels. En conséquence, à chaque niveau une théorie d'organisation de la SSII en vient à un besoin d'autonomisation de la réflexion et de l'action, ceci par rapport à un objectif de performance et de SSII globale lui-même constamment recherché-ajusté.

Avec le temps, le dirigeant n'est plus formé de la même manière que l'ingénieur de projet, que l'acteur opérationnel. Les deux ne sont plus reliés, comme deux univers séparés. Il y a d'une part évolution de la théorie des organisations et d'autre part la continuation de la question du perfectionnement des opérations de production de projets informatiques. On est dans une conceptualisation technique d'organisation déconnectée d'une partie des dirigeants, qui eux utilisent d'autres techniques d'organisation issues de théories. Il en résulte des problèmes de compétences disjointes et de cadres de pensées disjoints. Il y aurait alors confrontation entre deux trajectoires :

1) Celle qui émerge du terrain de la production industrielle informatique en

France, "sorte" de généralisation épistémologique par insistance qui deviendrait LE modèle généralisable (forme "initiale" SANS fondement épistémologique mais constante – manie ou toquade - et formerait LA norme) ;

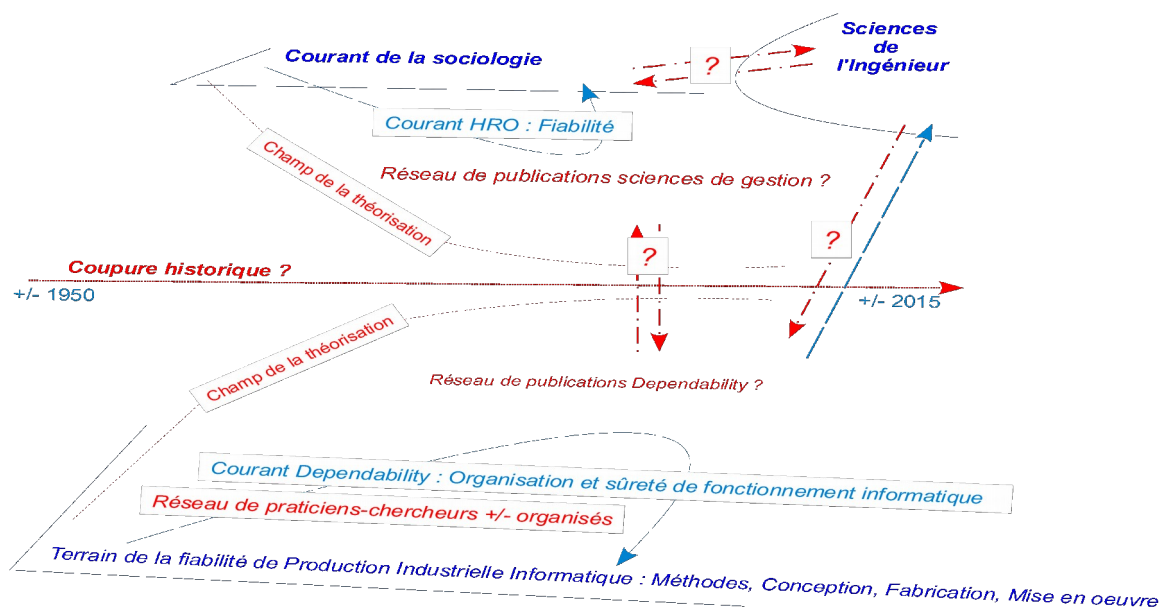
2) Ailleurs une série de modèles d'origine positiviste et leur utilisation managériale par laquelle ils sont diffusés comme LA référence de l'entreprise. La notion d'espérance est alors inversée au cours du temps au profit de la notion de risque.

Selon ce point de vue notre objet consiste alors à élaborer une méthodologie pour identifier ce que signifie « Coupure entre le courant de la HRO-fiabilité et celui de la Dependability des fonctionnalités SSI ».

3. Méthodologie

L'objet de notre méthodologie est d'établir les premiers fondements de notre démarche méthodologique pour ensuite répondre à ces questions d'identifications de paradigmes afin d'apporter quelque éclairage sur des nuances, liens ou non liens, entre courants.

Pour nous y aider, la figure ci-dessous représente la structure générale de notre hypothèse selon laquelle il y aurait une coupure historique, depuis les années 50, entre d'une part un courant de la sociologie, avec les Sciences de l'ingénieur, et, d'autre part un courant de la Dependability (Organisation et Sûreté de Fonctionnement), avec le Terrain de la fiabilité de Production industrielle informatique en France (Méthodes, Conception, Fabrication, Mise en Oeuvre). Chacun des courants serait identifiable par son réseau de publications. Pour chaque courant, une analyse de ses publications est une piste pour identifier son ou ses paradigmes, ses références à d'autres auteurs et publications.



Cou

pure entre HRO-fiabilité et Dependability -

Ces formes d'identifications et analyses de courants pourraient alors aider :

1. À préciser (voire à démontrer) en quoi les industriels peuvent dire qu'il n'y a pas de lien avec la HRO (alors montrons qu'il n'y en a pas), ou en quoi c'est plus compliqué (alors montrons le) ;
2. Mais aussi à vérifier :
 - 2.1. En quoi la coupure est liée aux écarts de réseaux de publications scientifiques (par ceux de la HRO-fiabilité (OHF), de la Dependability (SDF), des sciences de l'ingénieur) ;
 - 2.2. Si la coupure n'existe pas, alors en quoi les courants sont reliés.

Pour nous aider à préciser notre propos, « rappelons que le terme d'« épistémologie » vient du grec épistémê (connaissance, science) et de logos (« discours sur » mais aussi « logique de »), (Pesqueux, 2011, p. 3/24). » Ainsi notre objet est d'analyser chaque courant selon notre figure ci-dessus, au regard de son « discours sur » mais aussi de « logique de » connaissance dans son (et voire avec son ??) domaine. Pour cela on retient que par l'épistémologie l'on « étudie de manière critique la méthode scientifique, les formes logiques et modes d'inférence utilisés en science, de même que les principes, concepts fondamentaux, théories et résultats des diverses sciences, et ce, afin de déterminer leur origine logique, leur

valeur et leur portée objective, (Pesqueux, 2011, p. 3/24). »

En d'autres termes, par des analyses critiques de discours et de logique nous cherchons à identifier la(les) conception(s) théorique(s) dominante(s), c'est-à-dire le(s) paradigme(s) ayant cours à une certaine époque dans chaque courant. Nous analysons sur quoi et comment, de manière critique, la ou les méthodes, les formes logiques et modes d'inférence sont utilisés dans chacun de ces courants, tout ceci en vue d'identifier la (ou les) nuance(s) épistémologique(s) entre courants.

Avec JL. Lemoigne pour avancer dans notre compréhension de la nature des paradigmes identifiés alors, on essaie de répondre à trois questions liées à une épistémologie, (Pesqueux, 2011, p. 3/24) :

- Savoir ce qu'est la connaissance du domaine concerné (question gnoséologique) ; « cette perspective répond à la question « quoi ? » et conduit aux deux attitudes suivantes : celle qui considère l'organisation comme une « chose », d'ordre ontologique et celle qui conduit à considérer l'organisation comme un processus (d'ordre phénoménologique), (Pesqueux, 2011, p. 3/24). » Ici l'on essaie d'identifier l'idée de la « chose » et/ou celle du processus selon un point de vue de nuance de paradigmes ; ontologie vs phénoménologie ;
- Puis identifier comment un courant « s'est-il constitué ou engendré (question méthodologique) pour identifier un fondement, ou une raison de l'usage d'un paradigme. Cette perspective répond à la question « comment ? » Ici nous essayons de préciser la nature de notre paradigme, en vue de clarifier une nuance pouvant « différer selon l'attitude adoptée dans la réponse à la question gnoséologique », (Pesqueux, 2011, p. 3/24) » ;
- Ce qui nous conduit à identifier « comment apprécier sa valeur ou sa validité (question axiologique, pragmatique, téléologique et politico-éthique) ? Cette perspective répond à la question « pourquoi ? » et ouvre le champ d'appréciation de la validité de l'attitude adoptée dans la réponse à la question méthodologique et à celle des valeurs associées suivant la réponse apportée à la question gnoséologique, (Pesqueux, 2011, p. 3/24). »

Ces courants sont conçus et développés par des acteurs qui s'expriment par voies

orales et écrites. Les écrits forment des documents où ces acteurs y expriment leurs discours et logiques (de conception et de développement). De tout cela une expression, forme d'histoire se déroule. C'est à partir de ces écrits que nous cherchons à clarifier plus encore des paradigmes (voire à en identifier d'autres).

En effet, les histoires individuelles fournissent des renseignements sur les mêmes individus à différents moments de leur expérience. L'information peut être recueillie au cours du temps, à des instants proches des événements enregistrés ou en une seule fois de manière rétrospective ; selon un(des) instant(s) où l'on sollicite la mémoire de l'acteur enquêté, (Legrand, 2010).

4. Terrain

Nous disposons de travaux et publications de praticiens-chercheurs ainsi que de chercheurs depuis 1968, plus encore depuis 1980, sur le domaine de la Sécurité des Systèmes d'Information et des SSII plus encore depuis 20 ans.

Afin d'identifier l'évolution des phénomènes dans le temps, nous procédons aussi par analyse de données longitudinales, sur enquêtes tenant compte de la durée (Degenne, 2003, Legrand, 2010). Ceci consiste, par analyse de documents et par entretiens, à identifier une logique de concepts et de pratiques organisationnelles.

5. Premiers résultats

Dans l'une de nos bases de données de plusieurs centaines de documents, issus d'un congrès internationale de Maîtrise des Risques - Sûreté de Fonctionnement (Lambdamu, repère LM19 pour l'année 2014, ayant lieu tous les deux ans en France), l'on recherche le(s) document(s) et une (ou des) partie(s) de leur texte comprenant une expression régulière (ici, de sécurité des systèmes) supposée aider à la recherche de paradigme, ainsi que la page concernée du document, afin de repérer les arguments qui pourraient servir à avancer dans l'identification d'un ou de plusieurs paradigmes de ce courant de Sûreté de fonctionnement en France.

Nous avons obtenu plusieurs dizaines de parties de textes associés aux termes recherchés et en cours d'analyse détaillée.

« Si des transformations peuvent offrir de véritables opportunités, elles ne sont pas sans conséquences sur la maîtrise des risques, » pour ce qui concerne la

Sécurité des Systèmes Industriels Interconnectés, « *il n'est plus possible de se limiter à une vision des risques à un moment donné.* » Nous en venons « *au contraire à imaginer des évolutions possibles des technologies, des contextes, des cultures, des organisations conduisant à transformer, voire à faire apparaître de nouveaux dangers ou de nouvelles opportunités en les projetant dans un horizon d'avenir incertain,* » (Lardeux, 2015, p. 2/6).

6. Quelques références

1. Ambil Ferrand (Laurence), 2014 - *Les HRO, quel apport pour la gestion du risque bancaire ? Le cas de « l'affaire Kerviel »* - Laurence Ambil Ferrand , GREDEG UMR-CNRS 7321 - 250 avenue Albert Einstein - Sophia Antipolis
2. Arlat (Jean) et al., 2006 – *Tolérance aux fautes* - Arlat (Jean), Yves Crouzet, Yves Deswarte, Jean-Charles Fabre, Jean-Claude Laprie, David Powell - Dans « Encyclopédie de l'informatique et des systèmes d'information », (J. Akoka and I. Comyn-Wattiau, Eds.),1-Références Partie 1 : La dimension technologique des systèmes d'information - Section 2 : L'architecture et les systèmes (M. Banâtre, Ed.), pp. 240-270 ISBN 27117-4846-4, Vuibert, Paris, France, 2006.
3. Artaza Abaroa (Felipe), 2006 - *Connaissance, histoire, relations, travail, acteurs, mutation* - L'histoire de la connaissance contemporaine : un éclairage pour la compréhension des relations de travail et le repositionnement des acteurs dans un monde en mutation - Revue internationale sur le travail et la société, février Felipe Artaza Abaroa, GREDEG, Université de Nice-Sophia Antipolis -
4. Avizienis (Algirdas) et al., 2004 - '*Basic Concepts and Taxonomy of Dependable and Secure Computing*', IEEE Trans. on Dependable and Secure Computing, vol. 1, no. 1, Jan-March 2004, pp. 11-33 - Source : Sûreté de fonctionnement informatique : concepts, défis, directions - Jean-Claude Laprie - ACI Sécurité et Informatique - Toulouse, 15-17 novembre 2004
5. Avizienis (Algirdas), Laprie (Jean-Claude), 2004 - *Fundamental Concepts of Dependability* - Algirdas Avizienis, UCLA Computer Science Dept., Univ. of California, Los Angeles, USA, Jean-Claude Laprie, LAAS-CNRS, Toulouse France, Brian Randell, Dept. of Computing Science, Univ. of Newcastle upon Tyne, U.K. - UCLA CSD Report no. 010028 - LAAS Report no. 01-145 - Newcastle University Report no. CS-TR-739 – 2004
6. Basbøll (Thomas) , 2012 - *What makes organization ?* - WMO Working paper series N° 0.4, Thomas Basbøll , Department of organization, Copenhagen Business School, 2012 This paper can be downloaded free of charge at: <http://www.cbs.dk/Forskning/Institutter-centre/Projekter/What-Makes-Organization>
7. Bérard (Céline), 3 novembre 2009 – *Le processus de décision dans les systèmes complexes : une analyse d'une intervention systémique* – Université Paris-Deauphine, EDOGEST , DRM-CREPA , Université du Québec à Montréal, Écoles des sciences de la gestion : HAL Id: tel-00519068 ; <https://tel.archives-ouvertes.fr/tel-00519068>
8. Bierly et al., 1995 - *Culture and high reliability organizations : the case of the nuclear submarine*. Journal of Management. 21(4) : 639-656.

9. Boin (Arjen), 2008 - *Crisis Management – Sage Library in Business & Management – Volume III* - Arjen Boin (under the direction of), 2008 - ISBN: 978-1-84787-088-9 (set of three volumes)
10. Bréal (Michel) – Bailly (Anatole), 1918 – *Dictionnaire étymologique du latin* – neuvième édition – Librairie Hachette et Cie – 79 Boulevard Saint-Germain – Paris – 1918
11. Caire (Jean), **2014** - *Vers un cycle de vie de Sécurité globale pour les systèmes informatiques industriels* - 19 e Congrès de Maîtrise des Risques et Sûreté de Fonctionnement - Dijon 21-23 octobre 2014
12. Chapouille, de Pazzis - Masson & Cie, Éditeurs – 1968 - *Fiabilité des systèmes* - P. Chapouille & R. de Pazzis, préface de J.J. Baron - B.C.E. - Direction des études (Bull General Electric France) – Service Formation Technique - Edition octobre 1967)
13. Coutinho, 1964 - *Failure-Effect Analysis* - Transactions of the New York Academy of Sciences, Division of Engineering. New York: New York Academy of Sciences, 564–85
14. Dechy (Nicolas), Dien (Yves), Llorry (Michel), **2010** – *Pour une culture des accidents au service de la sécurité industrielle* - 17e Congrès de Maîtrise des Risques et de Sûreté de Fonctionnement 5-7 octobre 2010 La Rochelle
15. Degenne (Alain), 2003 - *Introduction à l'analyse des données longitudinales* - Alain Degenne - Directeur de recherche au CNRS – 2003
16. Deltort (Bruno) et al., 2014 - *Organisation à haute fiabilité (HRO), quelles pratiques opérationnelles ?* - Bruno Deltort, Mireille Bulot, Henri Fanchini - Centre National d'Etudes Spatiales - 52 rue Jacques Hillairet - 75612 Paris Cedex - SECTOR , 12 avenue du Québec , B.P. 636 Villebon sur Yvette , F-91965 COURTABOEUF CEDEX - ARTIS FACT, 6 Rue Lacépède , 75005 Paris
17. Denyer (David) et al., 2011 - *Exploring reliability in information systems programmes* – David Denyer, Elmar Kutsch, Elizabeth (Liz) Lee-Kelly, Mark Hall, 2011 - International Journal of Project Management, Cranfield University, Bristol University, Volume 29, Issue 4, May 2011, Pages 442-454
18. Eisenhardt, Kathleen M. 1993. *High reliability organizations meet high velocity environments : common dilemmas in nuclear power plants, aircraft carriers, and microcomputer firms*. In : Roberts, Karlene H., ed. *New challenges to understanding organizations*. New York : Macmillan : 117-136
19. Feigenbaum, 1961 - *Total quality control – 14.2 Reliability and Costs* – p. 405-406 - Feigenbaum – McGraw-Hill – Mladinska – Knjiga - 1961
20. Garandel (Sylvie), Périnet (Romuald), 2014 - *Élargir l'horizon des possibles en multipliant les points de vue : la pouvoir des marguerites !* - Romuald Périnet - GDF SUEZ - DRI / CRIGEN - Site du Landy - BP 33 - 361 avenue du Président Wilson - 93211 St-Denis La Plaine Cedex - Sylvie Garandel - ATRISc Paris - 27 avenue de l'Opéra - 75000 Paris - FRANCE
21. Gioia (Dennis A.), 2006 – *On Weick : An Appreciation* – Dennis A. Gioia , *Organization Studies* 2006; 27; 1709 , DOI: 10.1177/0170840606068349 - European Group for Organizational Studies - <http://www.sagepublications.com>
22. Haapanen Pentti, Helminen Atte, 2002 - *Failure mode and effects analysis of software-based*

- automation systems* - Haapanen Pentti, Helminen Atte – (VTT Industrial Systems) - STUK-YTO-TR 190 / August 2002)
23. Hernes (Tor), 2008 - *Understanding Organization as Process* – 200 pages - Tor Hernes (under the direction of), 2008, Norwegian School of Management
 24. Hervé Laroche, Véronique Steyer, 2012 - *L'apport des théories du sensemaking à la compréhension des risques & crises* – Les Cahiers de la Sécurité Industrielle – 2012-06 – Fondation pour une culture de sécurité industrielle – FonCSI
 25. Juran, 1995 - *A History of Managing for Quality*, ASQC Press, Milwaukee 1995, pp. 555-556, Juran Joseph editor
 26. Laprie (Jean-Claude), 1992 – *Dependable Computing and Fault Tolerant Systems*, Vol. 5 – *Dependability : Basic Concepts and Terminology* – 1992, Springer-Verlag/Wien, Austria, A-1238 Wien
 27. Lardeux (Emmanuel), **2015** – *Maîtriser les risques dans un monde en mouvement, Appel à Communications* – Institut pour la Maîtrise des Risques, Lambda Mu 20, 2015
 - 28.** Legrand, Claude , 2010 – *Dynamique stratégique des organisations sportives et mode de régulation* – Cnam, **2010**
 29. Levenson et al., **2009**, « *Moving Beyond Normal Accidents and High Reliability Organizations : A Systems Approach to Safety in Complex Systems* », *Organization Studies*, vol. 30, n° 2 & 3, 2009, pp. 227-249
 30. Lu 17 avril 2013 [http://www-history.mcs.st-andrews.ac.uk/Biographies/Walter Shewhart.html](http://www-history.mcs.st-andrews.ac.uk/Biographies/Walter%20Shewhart.html)
 31. Maurice Schwob et Guy Peyrache, 1969 - *Traité de fiabilité* - Maurice Schwob et Guy Peyrache - Masson & Cie, Éditeurs - 1969, p. 4
 32. Melkonian (Tessa), Thierry Picq, 2009 - NUMÉRO 2009/05 p. 4 / 29 - *Collective performance of teams operating at the extreme : The case of Special Forces* - Tessa Melkonian, EM Lyon Business School, Thierry Picq, EM Lyon Business School, September 2009 - Article presented in EGOS, 2-4 July 2009, Barcelona
 33. Mispelblom (Frederik), 1995 - p. 31 - *Au-delà de la qualité* - Frederik Mispelblom - Syros alternatives sociologiques - 1995 - Naves, 19460
 34. Muret (Arnaud) - 2003, page 54/295 - *La Qualité en recherche : la construction d'une norme française* - Arnaud Muret - ENSMP/CSI/AM/2003
 35. Office of manned space flight, Appollo Program, NASA 1966 - *Procedure for Failure Mode, Effects, and Criticality Analysis (FMECA)* - August 1966 – Reproduced by National Technical Information Service US Department of Commerce Springfield, VA. 22161 – National Aeronautics and Space Administration - Washington, D.C. 20546
 36. Parthenay (Claude), 2005 - *Herbert Simon : rationalité limitée, théorie des organisations et sciences de l'artificiel* - CEPN (Paris XIII) & Université de Cergy-Pontoise
 37. Pesqueux (Yvon) , 2002 – *Organisations : modèles et représentations* – Puf – Vendôme – août 2002
 38. Pesqueux (Yvon), 2009 - *Technologie, technique et outils de gestion* - Manuscrit auteur, publié dans "Journée d'étude MTO, Montpellier : France (2009)" - <http://hal.archives->

39. Pesqueux (Yvon), 2010 – *De la transgression* – Yvon Pesqueux, Cnam, 2010
40. Pesqueux (Yvon), 2011 – *Pour une épistémologie des organisations* - <http://hal.archives-ouvertes.fr/hal-00510860/fr/>
41. Reifer, D.J., 1979 - *Software Failure Modes and Effects Analysis* - IEEE Transactions on Reliability, R-28, 3, pp. 247–249
42. Rochlin (Gene), 1993. *Defining high reliability organizations in practice : a taxonomic prologue*. In : Roberts, Karlene H., ed. *New challenges to understanding organizations*. New York : Macmillan : 11-32
43. Ruchlin, Hirsch S. 2004. *The role of leadership in instilling a culture of safety : lessons from the literature*. *Journal of Healthcare Management*. 49(1) : 47-58
44. Schulman (Paul). 1993b. *The negotiated order of organizational reliability*. *Administration and Society*. 25(3) : 353- 372
45. Shooman (Martin L.), 1990 - p. 3/702 – *Probabilistic Reliability : An Engineering Approach* – Second edition – Martin L. Shooman – Professor of Electrical Engineering and Computer Science, Polytechnic University – Robert E. Krieger Publishing Company – Malabar Florida – 1990
46. Simon (Leslie E.), 1965 - *The Stimulus of S.S. Wilks to Army Statistics* - Wilk's methodology - p. 1/7 - Leslie E. Simon - Major General, USA - 1965
47. Sutcliffe (Kathleen M.), Christianson (Marlys K.), 2012 – *Managing for the unexpected – Executive white paper* ; University of Michigan, Stephen M. Ross School of Business and University of Toronto, Rotman School of Management - This paper was summarized by Penelope Mallinckrodt (Ross MBA ' 13) based on chapter 64 of Cameron and Spreitzer's (Eds.) - *The Oxford Handbook of Positive Organizational Scholarship* (2012)
48. Thomas, Marlin U., 2006 - *Reliability and Warranties: Methods for Product Development and – Quality Improvement* - CRC, New York, 2006 – selon *A Short History of Reliability* – p. 1 / 7 James McLinn CRE, ASQ Fellow - April 28, 2010
49. Tillement (Stéphanie), 2011, p. 65/551 - *La sécurité en action dans les projets de modernisation d'installations ferroviaires. Etude du rôle des dynamiques intra et inter – groupes professionnels dans la maîtrise des risques* – Université de Grenoble - selon source M. Bourrier - 2001, 2003 - BOURRIER, M., (2001), *Organiser la fiabilité*, L'Harmattan, Collection Risques collectifs et situations de crise, Paris, France. - BOURRIER, M., (2003a), *La fiabilité organisationnelle : morceaux choisis d'un état des lieux*. In Gilbert, C. (Dir.), *Risque collectifs et situations de crises. Apports de la recherche en sciences humaines et sociales*. Paris : L'Harmattan, pp. 199-215
50. Vaujany (François-Xavier de), 2011 - *An Historically-Grounded Critical Analysis of Research Articles in IS* - *European Journal of Information Systems* 20, 4 (2011) 1-23 : <http://hal.archives-ouvertes.fr/hal-00644398/fr/> François-Xavier de Vaujany, 2011, Université Paris-Dauphine
51. Vidaillet (Bénédicte) et al., 2003, 2013 – *Le sens de l'action* – institut VITAL ROUX, Vuibert - Bénédicte Vidaillet (coordonné par), Florence Allard-Poesi, Gérard Koenig, Hervé Laroche, Christophe Roux-Dufort – 12100 Millau – décembre 2013

52. Weber (Klaus), Glynn (Mary Ann), 2006 – *Making sense with institutions : thought and action in Karl Weick's theory*– Organization Studies -Boston College, Northwestern University, USA, 2006 – 27(11) : 1639–1660 - ISSN 0170–8406 - Copyright © 2006 - SAGE Publications (London, Thousand Oaks, CA & New Delhi) www.egosnet.org/os DOI : 10.1177/0170840606068343
53. Weick (Karl E.) et al., 2014 - *The affective foundations of high-reliability organizing* - Journal of Organizational Behavior - Vanderbilt University, Lehigh University, University of Michigan - May 2014
54. Weick (Karl E.) et al. 1999 - *Organizing for High Reliability: Processes of Collective Mindfulness* - 30. Weick (Karl E.), Kathleen M. Sutcliffe and David Obstfeld - Source: R.S. Sutton and B.M. Staw (eds), Research in Organizational Behavior, Volume 1 (Stanford: - Jai Press, 1999), pp. 81–123
55. Weick (Karl E.), 1985. *The significance of corporate culture*. In : Frost, Peter J. ; Moore, Larry F. ; Louis, Meryl R. ; Lunberg, Craig C. ; Martin, Joanne, eds. Organizational culture. Newberry Park, CA : Sage : 381-389.
56. Weick (Karl E.), 1987. *Organizational culture as a source of high reliability*. California Management Review. 29(2) : 112-127.
57. Weick (Karl E.), 1991. *The vulnerable system : an analysis of the Tenerife air disaster*. In : Frost, Peter J. ; Moore,
58. Weick (Karl E.), 2007 - *The generative properties of richness* - 30. Weick (Karl E.), University of Michigan - Academy of Management Journal - 2007, Vol. 50, No. 1, 14–19
59. Weick (Karl E.), Karlene H. Roberts, 1993. *Collective mind in organizations : heedful interrelating on flight decks*. Administrative Science Quarterly. 38 : 357-381
60. Weick (Karl E.), Sutcliffe (Kathleen) – 2007 - *Managing the unexpected : resilient performance in an age of uncertainty*. 2nd ed. San Francisco: Jossey-Bass. 224 p
61. Wright (Vita), Missoula, Gregory Larson, Cade Spaulding, Kelly Rossetto, Georgi Rausch, Stephanie Durnford, September 2007 - *Using Social Science to Understand and Improve Wildland Fire Organizations : An Annotated Reading List* - Aldo Leopold Wilderness Research Institute, MT & Rocky Mountain Research Station, U.S. Department of Agriculture, Forest Service, University of Montana Missoula, MT, lxiiiSchulman, Paul. R. 1993a. The analysis of high reliability organizations : a comparative framework. In : Roberts, Karlene H., ed. New challenges to understanding organizations. New York : Macmillan : 33-54
62. Zio (Enrico) 2009, p. 6/52 - *Reliability engineering: Old problems and new challenges* - Reliability Engineering and System Safety, Elsevier, 2009, 94, pp.125-141. <hal-00610053>- p. 6/52 – source : Coleridge, S. T. (1983). Biographia Literaria. In J. Engell & W. J. Bate (Eds.), The collected works of Samuel Taylor Coleridge. New Jersey: Princeton University Press